Claims

1. A data handling apparatus for a computer platform using an operating system executing a process, the apparatus comprising a system call monitor for detecting predetermined system calls, and means for applying a data handling policy to the system call upon a predetermined system call being detected, whereby the data handling policy is applied for all system calls involving the writing of data outside the process.

2. A data handling apparatus according to claim 1, in which the policy is to require the encryption of at least some of the data.

3. A data handling apparatus according to claim 1, in which a policy interpreter in its application of the policy automatically encrypts the at least some of the data.

4. A data handling apparatus according to claim 1, in which predetermined system calls are those involving the transmission of data externally of the computing platform.

5. A data handling apparatus according to claim 1, in which the means for applying a data handling policy comprises a tag determiner for determining any security tags associated with data handled by the system call, and a policy interpreter for determining a policy according to any such tags and for applying the policy.

6. A data handling apparatus according to claim 5, in which the policy interpreter is configured to use the intended destination of the data as a factor in determining the policy for the data.

7. A data handling apparatus according to claim 5, in which the policy interpreter comprises a policy database including tag policies and a policy reconciler for generating a composite policy from the tag policies relevant to the data.

8. A data handling apparatus according to claim 1, in which the computing platform comprises a data management unit, the data management unit arranged to associate data management information with data input to a process, and regulate operating system operations involving the data according to the data management information.

9. A data handling apparatus according to claim 8, in which the computing platform further comprises a memory space, and is arranged to load the process into the memory space and run the process under the control of the data management unit.

10. A data handling apparatus according to claim 8, in which the data management information is associated with at least one data sub-unit as data is input to a process from a data unit comprising a plurality of sub-units.

11. A data handling apparatus according to claim 8, in which data management information is associated with each independently addressable data unit.

12. A data handling apparatus according to claim 8, in which the data management unit comprises part of an operating system kernel space.

13. A data handling apparatus according to claim 12, in which the operating system kernel space comprises a tagging driver arranged to control loading of a supervisor code into the memory space with the process.

14. A data handling apparatus according to claim 13, in which the supervisor code controls the process at run time to administer the operating system data management unit.

15. A data handling apparatus according to claim 14, in which the supervisor code is arranged to analyse instructions of the process to identify operations involving the data, and, provide instructions relating to the data management information with the operations involving the data.

16. A data handling apparatus according to claim 13, in which the memory space further comprises a data management information area under control of the supervisor code arranged to store the data management information.

17. A data handling apparatus according to claim 8, in which the data management unit comprises a data filter to identify data management information associated with data that is to be read into the memory space.

18. A data handling apparatus according to claim 8, in which the data management unit further comprises a tag

management module arranged to allow a user to specify data management information to be associated with data.

19. A data handling apparatus according to claim 8, in which the data management unit comprises a tag propagation module arranged to maintain an association with the data that has been read into the process and the data management information associated therewith.

20. A data handling apparatus according to claim 19, in which the tag propagation module is arranged to maintain an association between an output of operations carried out within the process and the data management information associated with the data involved in the operations.

21. A data handling apparatus according to claim 19, in which the tag propagation module comprises state machine automatons arranged to maintain an association between an output of operations carried out within the process and the data management information associated with the data involved in the operations.

22. A data handling method for a computer platform using an operating system executing a process, the method comprising the steps of: detecting predetermined system calls, and applying a data handling policy to the system call upon a predetermined system call being detected, the data handling policy being applied for all system calls involving the writing of data outside the process.

23. A data handling method according to claim 22, in which the policy is to require the encryption of at least some of the data.

24. A data handling method according to claim 23, in which in its application of the policy at least some of the data is automatically encrypted.

25. A data handling method according to claim 22, in which predetermined system calls are those involving the transmission of data externally of the computing platform.

26. A data handling method according to claim 22, in which the method includes the steps of: determining any security tags associated with data handled by the system call, determining a policy according to any such tags and applying the policy.

27. A data handling method according to claim 26, in which a composite policy is generated from the tag policies relevant to the data.

28. A data handling method according to claim 26, in which the intended destination of the data is used as a factor in determining the policy for the data.

29. A data handling method according to claim 22, in which the method further comprises the steps of: (a) associating data management information with data input to a process; and (b) regulating operating system operations involving the data according to the data management information.

30. A data handling method according to claim 29, in which supervisor code administers the method by controlling the process at run time.

31. A data handling method according to claim 29, in which the step (a) comprises associating data management information with data as the data is read into a memory space.

32. A data handling method according to claim 29, in which the step (a) comprises associating data management information with at least one data sub-unit as data is read into a memory space from a data unit comprising a plurality of data sub-units.

33. A data handling method according to claim 29, in which the step (a) comprises associating data management information with each independently addressable data unit that is read into the memory space.

34. A data handling method according to claim 29, in which the data management information is written to a data management memory space under control of the supervisor code.

35. A data handling method according to claim 34, in which the supervisor code comprises state machine automatons arranged to control the writing of data management information to the data management memory space.

36. A data handling method according to claim 29, in which the step (b) comprises sub-steps (b1) identifying an operation involving the data; (b2) if the operation involves the data and is carried out within the process, maintaining an association between an output of the operation and the data management information; and (b3) if the operation involving the data includes a write

operation to a location external to the process, selectively performing the operation dependent on the data management information.

37. A data handling method according to claim 36, in which, the step (b1) comprises: analysing process instructions to identify operations involving the data; and, providing instructions relating to the data management information with the operations involving the data.

38. A data handling method according to claim 29, in which the process instructions are analysed as blocks, each block defined by operations up to a terminating condition.

39. A computer program for controlling a computing platform to operate in accordance with claim 22.

40. A computer platform configured to operate according to claim 22.

41. A data handling apparatus for a computer platform using an operating system executing a process, the apparatus comprising a system call monitor for detecting predetermined system calls, and a policy applicator for applying a data handling policy to the system call upon a predetermined system call being detected, whereby the data handling policy is applied for all system calls involving the writing of data outside the process.